(54) Title: SMARTCARD INTERNET AUTHORIZATION SYSTEM

(57) Abstract: A system and method are disclosed for conducting electronic commerce such as a virtual purchase transaction with an on-line merchant. A user is provided with an intelligent token, such as a smart card containing a digital certificate. The intelligent token suitably authenticates with a wallet server on a network that conducts all or portions of the transaction on behalf of the user without requiring changes to the merchant's server. The wallet server interacts with a security server of a selected financial service to provide authentication of the transaction. Upon authentication, the digital wallet prefills forms which are transmitted to the merchant who contacts the security server for validation of the forms and upon validation, completes the transaction with the user.

For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

SMARTCARD INTERNET AUTHORIZATION SYSTEM

FIELD OF THE INVENTION

The invention relates generally to methods and apparatus for conducting network transactions, and more particularly, to systems for

5   authenticating and conducting business over data networks such as the Internet.

BACKGROUND OF THE INVENTION

In recent years, many consumers have discovered the convenience and economy of purchasing goods and services electronically. A number of

10   channels for electronic purchases (commonly called "e-purchases") are available, including shop-at-home television networks, call-in responses to television advertisements, and the like. Most recently, direct purchasing via the Internet has become extremely popular.

In a typical Internet transaction, a consumer generally identifies goods

15   and/or services for purchase by viewing an online advertisement such as a hypertext markup language (HTML) document provided via a World Wide Web (WWW) browser. Payment typically occurs in various ways. One such way is via a charge card number that is provided via a secure channel such as a secure sockets layer (SSL) connection that is established between the

20   consumer and the merchant.

While millions of such transactions take place every day via the Internet, these conventional SSL transactions often exhibit a number of marked disadvantages. Although SSL typically provides a secure end-to-end connection that prevents unscrupulous third parties from eavesdropping (e.g.,

25   "sniffing") or otherwise obtaining a purchaser's charge card number, the protocol does not provide any means for ensuring that the charge card number itself is valid, or that the person providing the card number is legally authorized to do so. Because of the high incidence of fraud in Internet transactions, most charge card issuers consider network transactions to be

30   "Card Not Present" transactions subject to a higher discount rate. Stated another way, because of the increased risk from "Card Not Present"

transactions, most charge card issuers charge the merchant a higher rate for accepting card numbers via electronic means than would be charged if the card were physically presented to the merchant.

To improve the security deficiencies inherent in transporting charge card numbers over unsecure networks, many have suggested the use of "smart cards". Smartcards typically include an integrated circuit chip having a microprocessor and memory for storing data directly on the card. The data can correspond to a cryptographic key, for example, or to an electronic purse that maintains an electronic value of currency. Many smart card schemes have been suggested in the prior art, but these typically exhibit a marked disadvantage in that they are non-standard and typically require the merchants to obtain new, proprietary software for their Web storefronts to accept the smart card transactions. Moreover, the administration costs involved with assigning and maintaining the cryptographic information associated with smart cards have been excessive to date.

Another standard, the Secure Electronic Transaction (SET) standard has been suggested to improve the security of Internet transactions through the use of various cryptographic techniques. Although SET does provide improved security over standard SSL transactions, the administration involved with the various public and private keys required to conduct transactions has limited SET's widespread acceptance. SET also requires special software for those merchants wishing to support SET transactions.

Additionally, existing digital wallet technology, such as the digital wallet technology provided by, for example, GlobeSet, Inc., 1250 Capital of Texas Highway South, Building One, Suite 300, Austin, TX, 78746, is being more frequently used to provide a means for users to utilize transaction card products (e.g., credit, charge, debit, smart cards, account numbers and the like) to pay for products and services on-line. In general, digital wallets are tools which store personal information (name, address, chargecard number, credit card number, etc.) in order to facilitate electronic commerce or other network interactions. The personal information can be stored on a general server or at a client location (PC or Smartcard) or on a hybrid of both a general server and a client server. Presently, the digital wallet general server is comprised of a Web server and a database server which centrally houses

the user's personal and credit card information, shopping preferences and profiles of on-line merchants.

A digital wallet preferably performs functions such as single sign on/one password, automatic form filling of check out pages, one or two click
5   purchasing, personalization of Websites, on-line order and delivery tracking, itemized electronic receipts, and customized offers and promotions based upon spending patterns and opt-ins. More particularly, a one-click purchase activates the wallet and confirms the purchase at the same time. A two-click check out first activates the wallet, then the second click confirms the
10   purchase. In use, the wallet bookmark is typically clicked by the user and an SSL session is established with the Wallet server. A browser plug-in is executed and the user supplies an ID/password or smart card for authentication in order to gain access to the wallet data. When shopping at an on-line merchant, the appropriate wallet data is transferred from the wallet
15   server to the merchant's Web server.

Existing systems, however, generally require that a merchant initiate changes to accommodate each different smart card or wallet. Accordingly, a new system of conducting electronic transactions is desired which would provide improved security with minimal overhead for users and merchants.
20   Moreover, such a new system should integrate well with various smart cards and Internet wallets and other services provided by various merchants without requiring the merchant to make substantial changes to permit use of different systems.

SUMMARY OF THE INVENTION

25   In an exemplary embodiment of the invention, a user is provided with a smart card having a standardized protocol to make credit and debit transactions, such as, for example, the Blue™ from American Express™ smart card or the Europay MasterCard™ Visa™ (EMV) smart card. The user, also known as the cardmember (CM), utilizes the EMV Smartcard to interface
30   with a wallet server to authenticate the user with a merchant server on a network through communications with a security server provided by a financial institution or credit provider such as, for example, American Express (AMEX). The CM purchaser conducts a virtual purchase transaction via the internet

through a wallet server interacting with the security server to provide enhanced reliability and confidence in the transaction.

The user logs onto the internet via a browser and selects a wallet, causing the establishment of a secure sockets layer link to the wallet server and, at about the same time, activates the client window. The wallet server requests the user to insert the smartcard for authentication to the server wallet account. With an encrypted identity certificate being set, the user then selects the credit provider/financial institution, such as AMEX, who will be providing guarantee of the payment, from the provider available in the wallet. The user then logs onto the merchant server, completes shopping, goes to the checkout screen and clicks secure checkout. Again, the interfaces are over a secure sockets layer.

Next, the wallet server completes the form and transmits it to the merchant server, which uses telephone connections via a modem, direct link to a third party processor or directly to the security processor of the credit provider. The credit provider security processor uses the wallet interface to the user card to access smartcard functionality and generates a signed transaction. Alternatively, the connection can also be used to securely update functionality as required. The AMEX security processor authorizes the transaction on a "card press" basis. The merchant server then integrates the authorization with the wallet server completed form received from the wallet server and successfully completes the transaction, informing the user that the transaction has been successfully completed.

Thus, electronic transactions, such as purchase transactions, are conducted by receiving a transaction request from a user at a wallet server, issuing a challenge to the user from the wallet server, receiving a response from the user based upon the challenge, processing the response to verify the transaction instrument, assembling credentials (including authorization for the electronic transaction), and interfacing with a security server to authenticate the transaction. The system provides the benefits of protecting the market and the credit provider from fraud, transaction non-imputation, an ability to modify parameters on-line, and providing the user with better service at a lower cost by reducing the costs to the merchant because the entire process is transparent to the merchant.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other features and advantages of the present invention are hereinafter described in the following detailed description of exemplary embodiments to be read in conjunction with the accompanying drawing figures, wherein like reference numerals are used to identify the same or similar parts or steps in the similar views, and:

Figure 1 is a block diagram of an exemplary embodiment of the transaction system of the present invention; and

Figure 2 is a diagram of an exemplary process executed by the exemplary transaction system of Figure 1.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

The present invention may be described herein in terms of functional block components and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the present invention may employ various integrated circuit (I.C.) components, e.g., memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, or the like, with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. Still further, the invention could be used to detect or prevent security issues with a scripting language, such as JavaScript, VBScript or the like. For a basic introduction of cryptography, please review a text written by Bruce Schneider which is entitled "Applied Cryptography: Protocols, Algorithms, And Source Code In C," published by John Wiley & Sons (second edition, 1996), which is hereby incorporated by reference.

It should be appreciated that the particular implementations shown and described herein are illustrative of the invention and its best mode and are not intended to otherwise limit the scope of the present invention in any way. Indeed, for the sake of brevity, conventional data networking, application

5   development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted

10   that many alternative or additional functional relationships or physical connections may be present in a practical electronic transaction system.

To simplify the description of the exemplary embodiment, the invention is described as pertaining to a system of electronic commerce, i.e., transactions, running over the Internet. It will be appreciated, however, that

15   many applications of the present invention could be formulated. For example, the system could be used to authenticate users of a computer system, or to activate a passcode system, or any other purpose. One skilled in the art will appreciate that the network may include any system for exchanging data or transacting business, such as the Internet, an intranet, an extranet, WAN,

20   LAN, satellite communications, and/or the like. Communication between the parties to the transaction and the system of the present invention is accomplished through any suitable communication means, such as, for example, a telephone network, Intranet, Internet, point of interaction device (point of sale device, personal digital assistant, cellular phone, kiosk, etc.),

25   online communications, off-line communications, wireless communications, and/or the like. The users may interact with the system via any input device such as a keyboard, mouse, kiosk, personal digital assistant, handheld computer (e.g., Palm Pilot®), cellular phone and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer,

30   network computer, workstation, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, or the like. Moreover, although the invention is frequently described herein as being implemented with TCP/IP communications protocols, it will be

readily understood that the invention could also be implemented using IPX, Appletalk, IP-6, NetBIOS, OSI or any number of existing or future protocols.

5   Furthermore, the user and merchant may represent individual people, entities, or business and while reference is made to AMEX, this is by way of example and the financial authorization entity may represent various types of card issuing institutions, such as banks, credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. The payment network includes existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other

10 types of financial/banking cards.

Additionally, other participants may be involved in some phases of the transaction, such as an intermediary settlement institution, but these participants are not shown. Each participant is equipped with a computing system to facilitate transactions. The user has a personal computer, the

15 merchant has a computer/server, and the financial authorization entity has a main frame computer; however, any of the computers may be a mini-computer, a PC server, a network set of computers, laptops, notebooks, hand held computers, set-top boxes, and the like.

The customer and merchant may represent individual people, entities,

20 or business. Although labeled as a "bank," the bank may represent other types of card issuing institutions, such as credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. It is further noted that other participants may be involved in some phases of the transaction, such as an intermediary settlement institution, but

25 these participants are not shown.

Each participant is equipped with a computing system to facilitate online commerce transactions. The customer has a computing unit in the form of a personal computer, although other types of computing units may be used including laptops, notebooks, hand held computers, set-top boxes, and

30 the like. The merchant has a computing unit implemented in the form of a computer-server, although other implementations are possible. The bank has a computing center shown as a main frame computer. However, the bank computing center may be implemented in other forms, such as a mini-computer, a PC server, a network set of computers, and the like.

The computing units are connected with each other via a data communication network. The network is a public network and assumed to be insecure and open to eavesdroppers. In the illustrated implementation, the network is embodied as the internet. In this context, the computers may or may not be connected to the internet at all times. For instance, the customer computer may employ a modem to occasionally connect to the internet, whereas the bank computing center might maintain a permanent connection to the internet. It is noted that the network may be implemented as other types of networks, such as an interactive television (ITV) network.

5

The merchant computer and the bank computer are interconnected via a second network, referred to as a payment network. The payment network represents existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards. The payment network is a closed network that is assumed to be secure from eavesdroppers. Examples of the payment network include the American Express®, VisaNet® and the Veriphone® network.

10

15

The electronic commerce system is implemented at the customer and issuing bank. In an exemplary implementation, the electronic commerce system is implemented as computer software modules loaded onto the customer computer and the banking computing center. The merchant computer does not require any additional software to participate in the online commerce transactions supported by the online commerce system.

20

A customer account number may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". The first five to seven digits are reserved for processing purposes and identify the issuing bank, card type and etc. In this example, the last sixteenth digit is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer.

25

30

Referring now to **Figure 1**, a transaction system 100 typically includes at least one user or cardmember (CM) having a computer incorporating an

internet browser 110 adapted to interface with a data network. In an exemplary embodiment, transaction system 100 is used in electronic commerce to conduct purchase transactions. It will be appreciated that although the transaction system described herein is an electronic commerce

5   system, the present invention is equally applicable to various other electronic transaction systems. Specifically, the user system 110 is a purchaser or user which interfaces with a computer having an interface through data network 120 to a merchant server 130 and also to a digital wallet server 140.

The various computer systems and servers are interconnected as

10   appropriate by data network 120, which is any data network, such as the internet or other public or private data network. Other suitable networks 120 include the public switch telephone network (PSTN), wireless networks, corporate or university intranets, and the like. Additionally, merchant server 130 is coupled to a modem 150 which is in communication with a third party

15   processor (TPP) 160 which may be, but is not necessarily included, in the financial authorization entity secure processor 170. TPP 160 is further coupled to a virtual point of sale (POS) gateway processor 190 which is in the financial authorization entity secure processor 170. Also in the secure processor 170, and coupled to POS gateway processor 190, is payment

20   authorization gateway 180. Further, wallet server 140 is coupled to merchant server 130 and to virtual point of sale (VPOS) gateway processor 190.

While an exemplary embodiment has been illustrated in **Figure 1**, it will be appreciated that other embodiments are possible. Thus, as also described —above, components (e.g., user 110, merchant 120, and wallet server 140)

25   may be individual computers or network groups of computers acting with similar purpose to fulfill the functions described herein. Functionality attributed to a single component may be distributed among one or more individual computers in order to fulfill the described functionality. For example, the wallet server 140 may in fact be a collection of web servers,

30   application servers, data base servers, and other types of servers. Also, in various embodiments, data bases (not shown) and/or profile servers (not shown) may be connected to wallet server 140. For further information related to smart cards, browser functions, digital wallets and e-commerce transactions, see U.S. patent applications "Transaction Card", U.S. Serial No.

9/653,837, filed on September 1, 2000; "Method and Apparatus for Conducting Electronic Transactions", U.S. Serial No.: 09/652,899, filed on August 31, 2000; "System and Method For Authenticating A Web Page", U.S. Serial No. 09/656,074, filed on September 6, 2000; and, "System and Method

5   For Profiling A Web Site", U.S. Serial No. 09/656,061, filed on September 6, 2000, all of which are herein incorporated by reference.

To conduct a transaction, user 110 suitably establishes a connection through network 120 with a merchant 130. When a purchase is to be consummated, user 110 accesses wallet server 140. User 110 is then

10   directed by wallet server 140 to insert a Smart Card into the system to verify that a Smart Card is in the user's 110 possession. At the same time, a graphical representation of wallet 140 appears to the user 110 and user 110 is directed to select a transaction authorization entity, such as American Express (AMEX). The Smart Card preferably includes a digital certificate that

15   uniquely identifies the card such that digital credentials relating to the transaction may be created as described hereinafter. Upon receipt of the Smart Card information, wallet server 140 communicates with virtual POS gateway 190. Virtual gateway 190 queries payment authorization gateway 180 to obtain authorization for the payment. Upon obtaining such

20   authorization, virtual POS gateway transmits the information to wallet server 140. Wallet server 140 then completes an authorization form and transmits the form to merchant server 130.

Upon receipt of the authorization form, merchant server via modem 150 communicates with third party processor 160, which in turn

25   communicates with virtual POS gateway 190, again querying payment authorization gateway 180. Again, virtual POS gateway 190 communicates through third party processor 160 via modem 150 to merchant server 130, authenticating the completed form. Once completed, merchant server 130 authorizes the transaction and the transaction is completed, and the user 110

30   is notified.

Referring also to **Figure 2**, the flowchart shows an exemplary sequence of events involved in the on-line virtual transaction. As shown at step (210), a virtual transaction purchase by a customer is begun on-line, with a customer communicating with a vendor. At the completion of shopping, the

customer or user 110 initiates a secure checkout procedure as shown in step (220), opening the wallet and interfacing a Smart Card with the wallet server 140, including selecting the credit supplier. The wallet server 140 interfaces at step (220) with a security server to authenticate the transaction. In step

5 (240), the wallet server 140 receives transactional authentication, completes an authorization form for the transaction and transmits the form to the merchant server 130. In step (250), the merchant server queries the security server for credit supplier authentication of the authorization form. Based on the information supplied by the credit supplier, and in conjunction with the

10 authentication above discussed in the previous steps, the credit supplier authenticates the authorization form based on the information from the Smart Card provided through the wallet server and transmits an authentication to the merchant server 130. Upon receipt of the authorization form, the merchant completes the virtual transaction/purchase, informing the customer and

15 debiting the customer's account.

Because the Smart Card as above-described contains identifying information that is unique to a particular card, the purchase transaction conducted with the Smart Card is more secure than a transaction conducted with an ordinary charge or credit card. Accordingly, a discount rate may be

20 justified for the secure transaction, which may be processed by the card issuer as a "card present" transaction. Additionally, if the transaction is a "card present" transaction, risk of fraud may be transferred from the merchant to the card issuer.

Thus, the present invention is directed to a system and method for

25 permitting the authentication of a virtual on-line transaction where a user, by the use of a Smart Card and a wallet server, may have on-line virtual transactions authenticated to a merchant using various Smart Cards and credit providers while minimizing changes to the merchant's server to accommodate a number of different types of systems.

30 Accordingly, corresponding structures, acts, and equivalents of all elements in the claims below are intended to include any structural material or acts for performing the functions in combination with other elements as specifically claimed. The scope of the invention should be determined by the

allowed claims and their legal equivalents, rather than by the examples given above.

CLAIMS

What is claimed is:

1.   1.   A method for conducting a transaction, the method comprising:

2.   a.   receiving a request to authenticate a transaction from a user at a

3.   server;

4.   b.   requiring the user to provide an instrument for verification;

5.   c.   receiving an instrument input response from the user based

6.   upon said requirement;

7.   d.   processing said instrument input as an input to a security

8.   processor;

9.   e.   assembling forms for the transaction, said forms comprising said

10.   security processor authorization of said input to said security processor;

11.   f.   providing said forms incident to said transaction and sending a

12.   request to said security processor for a second authorization of said forms;

13.   and

14.   g.   validating said transaction with said second authorization of said

15.   forms received from said security processor.

2.   The method of Claim 1 further directed to providing such transaction
validation for different combinations of instruments and security processors
without requiring changes to transaction processing by said merchant.

3.   The method of Claim 1, wherein the transaction is an electronic
purchase transaction.

4.   The method of Claim 3, wherein the electronic purchase transaction is
conducted using a digital wallet.

5.   The method of Claim 1, wherein the instrument is a smart card.

1 6.   A method for providing secure virtual transactions between a user and

2 a an on-line merchant without requiring changes at the merchants location,

3 the method comprising:

4   a.   developing a first query for transmission to a credit provider;

5   b.   receiving a response from said credit provider and transmitting

6 same to said merchant;

7   c.   said merchant querying said credit provider for authentication of

8 said credit provider response; and

9   d.   completing said virtual transaction using authorization from said

10 credit provider.

7.   The method of Claim 6 wherein said first query is developed by

opening a wallet and inputting information from a smart card.

8.   The method of Claim 6, further comprising developing a form from said

response from said credit provider and transmitting said form to said

merchant.

9.   The method of Claim 8, wherein said merchant requests authentication

of said form from said credit provider.

10.   The method of Claim 6, wherein said credit provider is selected by said

user from a group of credit providers.

11.   The method of Claim 9, wherein said credit provider is selected by said

user from a group of credit providers..

1 12.   A method for conducting a transaction, the method comprising:

2   a.   receiving a request to authenticate a transaction with a

3 merchant from a server;

4   b.   requiring an instrument for providing verification;

5   c.   receiving an instrument input response based upon said

6 requirement;

7   d.   processing said instrument input as an input to a security

8   processor;

9   e.   assembling forms for the transaction, said forms comprising said

10 security processor authorization of said input to said security processor;

11   f.   providing said forms incident to said merchant;

12   g.   said merchant processing said forms and sending a request to

13 said security processor for a second authorization of said forms; and

14   h.   validating said transaction with said second authorization of said

15 forms received from said security processor.

13.   The method of Claim 12, further directed to providing such transaction

validation for different combinations of instruments and security processors

without requiring changes to transaction processing by said merchant.

14.   The method of Claim 12, wherein the transaction is an electronic

purchase transaction.

15.   The method of Claim 14, wherein the electronic purchase transaction is

conducted using a digital wallet.

16.   The method of Claim 12, wherein the instrument is a smart card.

1   17.   A method for conducting a transaction, the method comprising:

2   a.   receiving a request to authenticate a transaction at a server;

3   b.   requiring an instrument for verification of said request;

4   c.——   receiving an instrument input response based upon said

5   requirement;

6   d.   processing said instrument input as an input to a security

7   processor;

8   e.   assembling forms for the transaction, said forms comprising said

9   security processor authorization of said input to said security processor;

10   f.   providing said forms for authorization;

11   g.   processing said forms and sending a request to said security

12 processor for a second authorization of said forms; and

13   h.   validating said transaction with said second authorization of said

14   forms received from said security processor.

18.   The method of Claim 17, further directed to providing such transaction validation for different combinations of instruments and security processors without requiring changes to transaction processing by said merchant.

19.   The method of Claim 17, wherein the transaction is an electronic purchase transaction.

20.   The method of Claim 19, wherein the electronic purchase transaction is conducted using a digital wallet.

21.   The method of Claim 17, wherein the instrument is a smart card.

1   22.   A method for conducting a transaction, the method comprising:

2   a.   receiving a request to authenticate a transaction with a

3   merchant from a user at a server;

4   b.   requiring the user to provide an instrument for verification;

5   c.   receiving an instrument input response from the user based

6   upon said requirement;

7   d.   processing said instrument input as an input to a security

8   processor;

9   e.   assembling forms for the transaction, said forms comprising said

10   security processor authorization of said input to said security processor;

11   f.   providing said forms to said merchant;

12   g.   said merchant processing said forms and sending a request to

13   said security processor for a second authorization of said forms; and

14   h.   validating said transaction with said second authorization of said

15   forms received from said security processor.

23.   The method of Claim 22, further directed to providing such transaction validation for different combinations of instruments and security processors without requiring changes to transaction processing by said merchant.

24.   The method of Claim 22, wherein the transaction is an electronic purchase transaction.

25.   The method of Claim 24, wherein the electronic purchase transaction is conducted using a digital wallet.

26.   The method of Claim 22, wherein the instrument is a smart card.

1   27.   A transaction system, comprising:
2   a.   a data network, including at least one instrument and operative
3   to permit initiation of a transaction;
4   b.   an authorization server coupled to receive said initiation of said
5   transaction as an input and transmit same to a security server;
6   c.   said security server operative to receive said input from said
7   authorization server and generate and transmit an authorization to said
8   authorization server;
9   d.   said authorization server coupled to receive said authorization
10   from said security server and operative to generate and transmit an
11   authorization form; and
12   e.   an interface coupled to said security server and operative to
13   permit validation of said form and complete a secure on-line virtual
14   transaction.

28.   The transaction system of Claim 27, further operative to provide said validation for different combinations of instruments and security processors.

29.   The transaction system of Claim 27, wherein said authorization server is an electronic purchase server.

30.   The transaction system of Claim 29, wherein said electronic purchase server is coupled to a digital wallet and operative to validate said transaction input transmitted to said security server.

1   31.   A transaction system, comprising:

2   a.   a data network operative to permit a user to initiate a

3   transaction;

4   b.   an authorization server coupled to receive an input from said

5   user and transmit same to a security server;

6   c.   said security server coupled to receive said input from said

7   authorization server and operative to generate and transmit an authorization

8   to said authorization server;

9   d.   said authorization server coupled to receive said authorization

10   from said security server and operative to generate and transmit an

11   authorization form; and

12   e.   an interface coupled to said security server and operative to

13   permit validation of said form and complete a secure on-line virtual transaction

14   with said user.

32.   The transaction system of Claim 31, further operative to provide said
form validation for different combinations of instruments and security
processors.

33.   The transaction system of Claim 31, wherein said authorization server
is an electronic purchase server.

34.   The transaction system of claim 33, wherein said electronic purchase
server is coupled to a digital wallet and operative to validate said user input
transmitted to said security server.

1   35.   A transaction system, comprising:

2   a.   a data network operative to permit initiation of a transaction with

3   a merchant;

4   b.   an authorization server coupled to receive said transaction

5   initiation as an input and transmit same to a security server;

6   c.   said security server coupled to receive said input from said

7   authorization server and operative to generate and transmit an authorization

8   to said authorization server;

9   d.   said authorization server coupled to receive said authorization

10   from said security server and operative to generate and transmit an

11   authorization form; and

12   e.   an interface coupled to said security server and operative to

13   permit validation of said form and complete a secure on-line virtual transaction

14   with said user.

36.   The transaction system of Claim 35, further operative to provide said validation for different combinations of instruments and security processors.

37.   The transaction system of Claim 35, wherein said authorization server is an electronic purchase server.

38.   The transaction system of Claim 37, wherein said electronic purchase server is coupled to a digital wallet and operative to validate said transaction input transmitted to said security server.
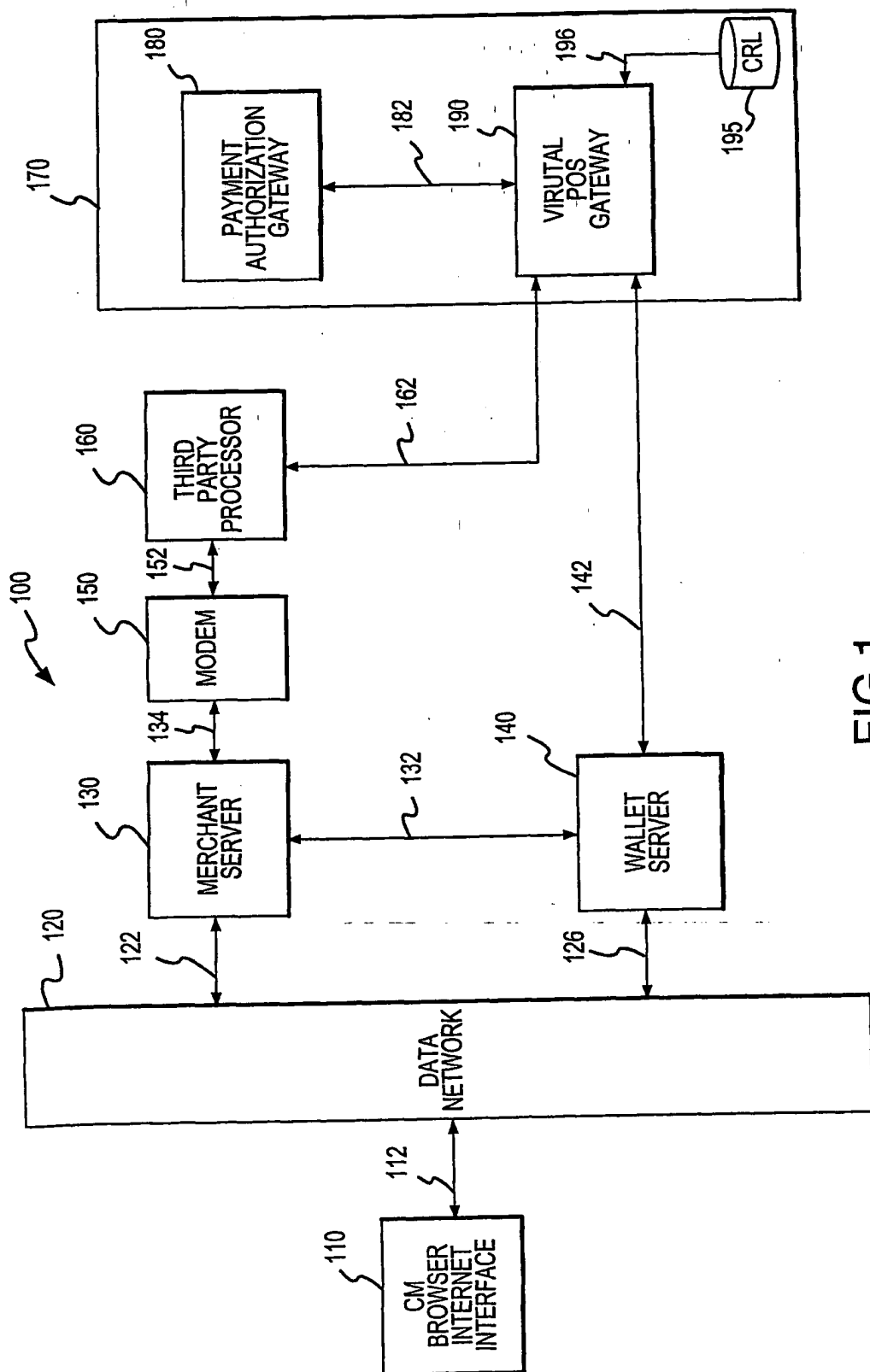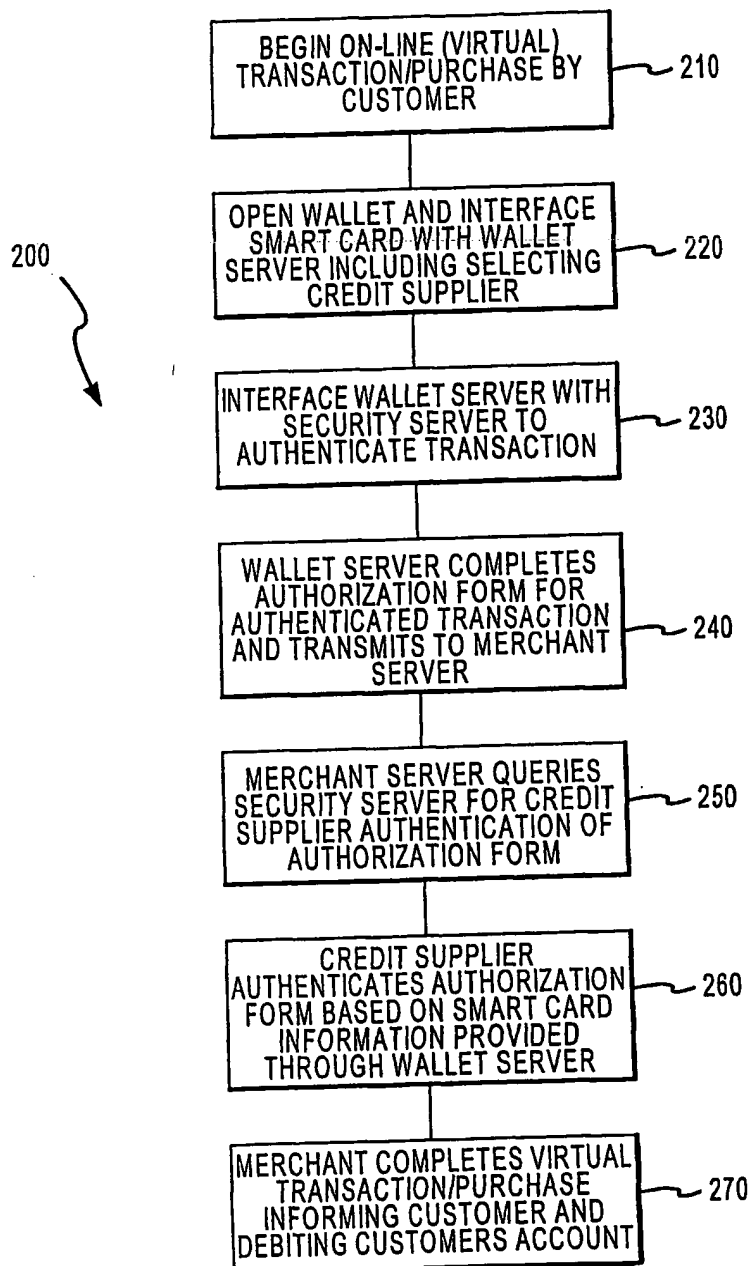
FIG.1

2/2

```
                    ┌──────────────────────┐
                    │ BEGIN ON-LINE (VIRTUAL)│
                    │ TRANSACTION/PURCHASE BY│──── 210
                    │      CUSTOMER          │
                    └──────────────────────┘
                              │
                    ┌──────────────────────┐
                    │ OPEN WALLET AND INTERFACE│
            200     │ SMART CARD WITH WALLET  │
                    │ SERVER INCLUDING SELECTING│──── 220
                    │    CREDIT SUPPLIER       │
                    └──────────────────────┘
                              │
                    ┌──────────────────────┐
                    │INTERFACE WALLET SERVER WITH│
                    │    SECURITY SERVER TO    │──── 230
                    │  AUTHENTICATE TRANSACTION │
                    └──────────────────────┘
                              │
                    ┌──────────────────────┐
                    │ WALLET SERVER COMPLETES │
                    │  AUTHORIZATION FORM FOR  │
                    │ AUTHENTICATED TRANSACTION│──── 240
                    │ AND TRANSMITS TO MERCHANT│
                    │       SERVER            │
                    └──────────────────────┘
                              │
                    ┌──────────────────────┐
                    │ MERCHANT SERVER QUERIES │
                    │ SECURITY SERVER FOR CREDIT│──── 250
                    │ SUPPLIER AUTHENTICATION OF│
                    │   AUTHORIZATION FORM     │
                    └──────────────────────┘
                              │
                    ┌──────────────────────┐
                    │   CREDIT SUPPLIER       │
                    │AUTHENTICATES AUTHORIZATION│
                    │ FORM BASED ON SMART CARD │──── 260
                    │  INFORMATION PROVIDED    │
                    │  THROUGH WALLET SERVER   │
                    └──────────────────────┘
                              │
                    ┌──────────────────────┐
                    │MERCHANT COMPLETES VIRTUAL│
                    │  TRANSACTION/PURCHASE    │──── 270
                    │ INFORMING CUSTOMER AND   │
                    │DEBITING CUSTOMERS ACCOUNT│
                    └──────────────────────┘
```

FIG.2

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   G07F 19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7   G07F   G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 883 810 A (ROSEN DANIEL ET AL) 16 March 1999 (1999-03-16) abstract; claims 1,7,21; figures 1-4	1-38
Y	US 5 978 840 A (SUBRAMANIAN MAHADEVAN P ET AL) 2 November 1999 (1999-11-02) abstract; figure 10 column 14, line 35 – line 45 column 26, line 55 – line 67	1-38
E	WO 01 15034 A (DIGITALCONVERGENCE COM INC) 1 March 2001 (2001-03-01) the whole document	1-38
A	EP 0 926 637 A (NIPPON TELEGRAPH & TELEPHONE) 30 June 1999 (1999-06-30) abstract; claim 1; figure 1 column 4, line 37 –column 5, line 22	1-38

-/--

[X] Further documents are listed in the continuation of box C.   [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 June 2001	13/06/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Guivol, O

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 903 721 A (SIXTUS TIMOTHY) 11 May 1999 (1999-05-11) column 6, line 33 -column 11, line 35; figures	1-38
A	EP 0 927 945 A (AMAZON COM INC) 7 July 1999 (1999-07-07) the whole document	1-38
A	US 5 500 890 A (COOPER CHRISTOPHE K ET AL) 19 March 1996 (1996-03-19) column 3, line 51 -column 4, line 16; figure 3	1,6,12, 17,22, 27,31,35
A	EP 0 813 325 A (AT & T CORP) 17 December 1997 (1997-12-17) the whole document	1,3,6, 8-12,14, 17,22, 27,31,35

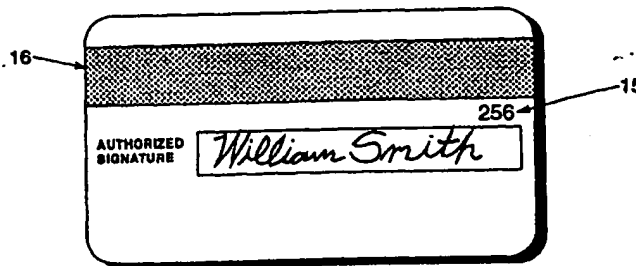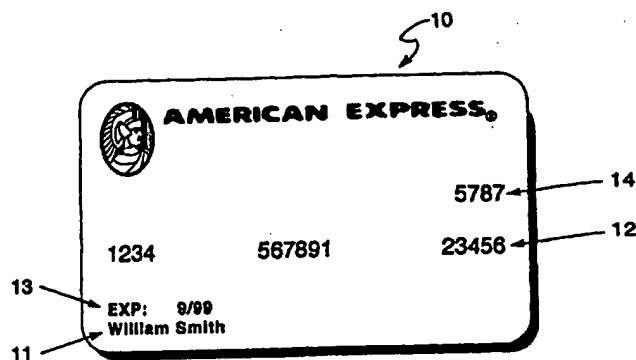| Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5883810	A	16-03-1999	NONE		
US 5978840	A	02-11-1999	AU 4654497 A		17-04-1998
			EP 0929881 A		21-07-1999
			WO 9813797 A		02-04-1998
WO 0115034	A	01-03-2001	NONE		
EP 0926637	A	30-06-1999	JP 11265417 A		28-09-1999
US 5903721	A	11-05-1999	AU 6549498 A		29-09-1998
			DE 1008022 T		25-01-2001
			EP 1008022 A		14-06-2000
			ES 2150892 T		16-12-2000
			NO 994428 A		09-11-1999
			WO 9840809 A		17-09-1998
EP 0927945	A	07-07-1999	US 5960411 A		28-09-1999
			AU 9477998 A		29-03-1999
			CA 2246933 A		12-03-1999
			CA 2263781 A		12-03-1999
			EP 0902381 A		17-03-1999
			JP 11161717 A		18-06-1999
			JP 2000099592 A		07-04-2000
			WO 9913424 A		18-03-1999
US 5500890	A	19-03-1996	NONE		
EP 0813325	A	17-12-1997	US 5778173 A		07-07-1998
			CA 2205124 A		12-12-1997
			JP 10149397 A		02-06-1998

PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 19/06	A1	(11) International Publication Number: WO 00/25262
		(43) International Publication Date: 4 May 2000 (04.05.00)

(21) International Application Number: PCT/US99/25423

(22) International Filing Date: 28 October 1999 (28.10.99)

(30) Priority Data:
09/181,734   28 October 1998 (28.10.98)   US

(71) Applicant: AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC. [US/US]; American Express Tower, World Financial Center, New York, NY 10285 (US).

(72) Inventors: HACKETT, Ann; 15263 South 24th Street, Phoenix, AZ 85048 (US). ARNOLD, Lisa; Building 10400, 10030 North 25th Avenue, Phoenix, AZ 85020 (US). JORDAN, Vickie; 4722 North 53rd Street, Phoenix, AZ 85018 (US).

(74) Agent: SOBELMAN, Howard, I.; Snell & Wilmer, L.L.P., One Arizona Center, 400 East Van Buren, Phoenix, AZ 85004–0001 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION CARD

(57) Abstract

Instead of a PIN which is associated with an account and provides access to an account, a card identification code (14), which is located on the card (10) but does not provide automatic access to an account, is used to verify that the consumer currently possesses the transaction card (10) at the time of purchase and/or is the true card owner. At the time of card printing, an embossing file of account codes (12) including associated identification codes is created and loaded into the account database. At the time of authorization, the identification code (14) and the account code (12) are entered into a POS device and sent to an authorization system. If the identification codes match, and other authorization parameters are satisfied, the transaction card is authorized.

SYSTEMS AND METHODS FOR AUTHORIZING A TRANSACTION CARD

BACKGROUND OF THE INVENTION

1. Technical Field

The present invention relates, generally, to transaction card fraud reduction
5 systems and methods and, more particularly, to verifying that a consumer is in possession
of a transaction card and/or is the true card owner during a purchase transaction.

2. Background Information

Transaction cards such as, for example, credit cards, debit cards, bank cards,
charge cards, smart cards and the like, have become increasingly popular for purchasing
10 goods and services and for conducting other transactions. A transaction card typically
includes information related to the issuer's name and logo, an account number, an
expiration date and the cardholder's name. The cards may also have other information,
serial number and/or the like printed on the card to represent other information about the
transaction card or about the card member such as, for example, a group number, a
15 promotion number, a card type number, a plastic issuance number and/or the like.
Certain information is often embossed on the card with raised print, thereby allowing the
information to be imprinted on a charge slip; however, the information that is unembossed
(flat) would not be imprinted onto the charge slip. For many transaction cards, the
information printed on the card is also contained within a magnetic stripe, a bar code
20 and/or an integrated circuit (microchip) for automatic downloading/reading by a card
reader.

Many card transactions are commenced by inserting, or sliding a card through, a
card reader which automatically downloads the card information, thereby allowing the
information to be used during the authorization process without the need for manual input
25 or review of the card information. However, because of the substantial increase in
fraudulent use and theft of transaction cards, the use of the card information is often
supplemented by various fraud prevention techniques, such as requiring a signature to
verify the consumer's agreement to the transaction or the entry of a PIN number to verify
the consumer's authority to use the transaction card. Additionally, certain card issuers,

such as banks, incorporate the consumer's picture onto the face of the transaction card to give the merchant an additional verification procedure.

While the use of a signature, PIN or picture is effective for fraud reduction when the cardholder presents a card to a merchant, these options are not as effective, and may not

5   be available, for other transactions. Particularly, transactions which do not require face-to-face contact between a consumer and merchant, such as the use of a transaction card to purchase items through the Internet or over the telephone (e.g., mail order). Moreover, many transactions may be alternatively completed without using the physical transaction card. For example, a consumer or merchant may simply key in the transaction card

10 number into the keypad of a POS device or the keypad on an ATM.

When conducting Internet, telephone or keypad transactions, a cardholder may only need to provide a card account number and expiration date to allow the merchant to charge a particular account and verify that the transaction card is valid. Other verification information, such as a PIN number, is usually not disclosed because the PIN

15 is typically memorized by the cardholder and never disclosed to anyone. Because merchants often only request limited information to conduct a transaction over the Internet or the telephone, an increased potential for fraud exists due to the increased availability of this general information. In other words, regardless of a consumer's possession of the physical transaction card, a consumer can still fraudulently obtain and provide this general

20 information.

Particularly, cardholders often provide a transaction card number to telemarketers, merchants, bank tellers and Internet sites, thereby allowing a merchant or clerk to retain the credit card number and associated information for later fraudulent use. Moreover, a person may overhear a transaction card number being disclosed over the telephone or,

25 with the increase of mailbox thefts, a person may obtain a credit card number from a billing statement or promotional literature. Furthermore, advanced computer operators are able to intercept transaction card numbers which are transmitted over modems and/or the Internet. Accordingly, when a merchant simply requests a credit card number from a consumer, it is difficult for the merchant to ensure that the consumer placing the order

30 has the transaction card in his or her possession and/or is the true cardmember, rather than using a stolen account number.

As stated above, the use of PIN numbers are typically limited to face-to-face or ATM transactions wherein the consumer personally enters a PIN into a keypad and the merchant does not need to have knowledge of the PIN. In non face-to-face transactions, the PIN would need to be disclosed to the merchant. However, due to security concerns,
5   consumers prefer to not disclose their private PIN number to merchants and especially prefer to not disclose the PIN number over a telephone or through the Internet. Particularly, a PIN number is directly associated with the account number, and as such, may provide increased access to a transaction card account during a fraudulent transaction. Accordingly, a system is needed which allows the consumer to disclose a
10 security number which is associated with the account number, but does not allow automatic access to the account.

BRIEF SUMMARY OF THE INVENTION

Due to security concerns during non face-to-face commercial transactions, consumers prefer to not disclose their private PIN number to merchants and especially
15 prefer to not disclose the PIN numbers over a telephone or through the Internet. Instead of a PIN which is associated with an account and provides access to an account, a card identification code, which is located on the card but does not provide automatic access to an account, is used to verify that the consumer currently possesses the transaction card at the time of purchase and/or is the true card owner.
20   Along with the account number, a transaction card includes a non-embossed four-digit or three-digit number, called a card identification code. During creation of a transaction card, a five-digit identification code is calculated from the account number, four-digit or three-digit identification code and the expiration date based upon a predetermined algorithm. A four-digit identification code is printed on the front of the card,
25 an associated five-digit identification code is entered into the magnetic stripe and an associated three-digit identification code is printed in the signature panel. An embossing file of account numbers including associated identification codes is created and loaded into the account database. At the time of authorization, the four-digit number on the front of the card and the account number are manually keyed into a POS device and sent to
30 an authorization system. The four-digit number is matched to the four-digit number on file

for that transaction card. If the four-digit numbers match, and other authorization parameters are satisfied, the transaction card is authorized.

Alternatively, when the card is swiped through a POS device, the five-digit number previously entered into the magnetic stripe, along with other information, is automatically

5 transmitted to the authorization system. The five-digit number is decomposed using a mathematical algorithm, and the resulting three-digit and/or four-digit numbers are matched against the database record (which includes the originally assigned three or four-digit identification codes for the account number). If the respective three or four-digit numbers match, and other authorization parameters are satisfied, the transaction card is

10 authorized.

Thus, the entry of an additional identification code helps verify that the consumer currently possesses the transaction card at the time of purchase or is the true card owner, rather than simply using a stolen account number. Accordingly, requiring entry of an identification code along with the account number provides an effective deterrent to

15 fraudulent use of the account number. For example, systems and methods in accordance with the present invention at certain tested locations have provided fraud reduction of approximately 78%.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

The subject invention will hereinafter be described in conjunction with the

20 appended drawing figures, wherein like numerals denote like elements, and:

Figure 1 is an exemplary flow diagram of the card creation and identification code creation process;

Figure 2a is a front view of an exemplary transaction card showing an account number and card identification code;

25   Figure 2b is a rear view of an exemplary transaction card showing magnetic strip and card identification code;

Figure 3 is an exemplary schematic diagram of a simplified transaction card authorization system;

Figure 4 is an exemplary schematic diagram of an authorization database with associated identification codes in accordance with an embodiment of the present invention; and,

Figure 5 is an exemplary flow diagram of the authorization process.

DETAILED DESCRIPTION OF THE INVENTION

5   To reduce fraud when conducting commercial transactions (i.e., the purchase of goods and services) using a transaction card 10, the present system requests entry of an additional number to help verify that the consumer has possession of the transaction card at the time of purchase or is the true card owner, rather than simply using a stolen

10   account code. Wherein a PIN number is typically memorized and not written down, the present number, called a card identification code 14, 15 and 16, is preferably printed on or encoded in transaction card 10. Due to security concerns during non face-to-face transactions, consumers prefer to not disclose their private PIN number to merchants and especially prefer to not disclose the PIN number over a telephone or through the Internet.

15   Instead of a PIN which is associated with an account and provides access to an account, a card identification code 14, 15 and 16, which does not provide automatic access to an account, is used to help verify that the consumer currently possesses the transaction card at the time of purchase and/or is the true card owner.

With momentary reference to Figure 2a, in accordance with the present invention,

20   a transaction card 10 includes any device suitably configured to display an account code 12 and a card identification code 14. In a preferred embodiment, the transaction card is a credit card, charge card, debit card, smart card, bank card and/or the like. Transaction card 10 preferably includes information for conducting a transaction. In a preferred embodiment, the front face of transaction card 10 includes an account code 12 and a card

25   identification code 14 located above account code 12. Account code 12 includes any number of characters (n characters) comprising any combination of numbers, letters, symbols or other indicia which are suitably configured to identify a transaction account. In a preferred embodiment, account code 12 is a 15-digit number which identifies an account code, including a routing number or other similar transaction numbers,

30   corresponding to the card owner. One of ordinary skill in the art will appreciate that

account code 12 may be associated with an individual account, a corporate account, an organization account, or any other entity and the account may represent a charge account, a credit account, a debit account, an electronic purse account, or any other financial account.

5   Card identification codes 14, 15 and 16 include any number of characters (n characters) comprising any combination of numbers, symbols, letters, or other indicia suitably configured to provide verification that the consumer has an actual card in possession at the time of purchase and/or is the true card owner, rather than simply using a stolen account code. In a preferred embodiment, card identification code 14 is printed

10 on or encoded in transaction card 10. Card identification code 14 may be located on either side of the card, encoded into a medium on the card and may be embossed (raised lettering) or unembossed (flat) into the plane of the card. In a particularly preferred embodiment, card identification code 14 is located on the front face of transaction card 10 on the same side as, and above, account code 12. Moreover, card identification code

15 14 is preferably a four-digit, unembossed (flat) number printed within the plane of the card. One skilled in the art will appreciate that, along with other card member information, card identification codes 14, 15 or 16 may be initially printed on many transaction cards 10 before, during or after account code 12 is printed on transaction card 10. In a preferred embodiment, card identification codes 14 or 15 are logically related to card

20 identification code 16.

      After a consumer is approved for a transaction card, an account code 12, a four-digit identification code 14 and/or a three digit code 15, an expiration date 13 and other information are associated with the consumer's name in an account database 30 (see Figures 2a and 3). With reference to Figures 1 and 3, account code 12, a four-digit

25 identification code 14 (or a three-digit identification code 15), an expiration date 13 and other information from account database 30 are preferably transmitted to a card creation system 32 (step 38). In a preferred embodiment, at the time of creating transaction card 10 for the consumer in accordance with the present invention, a five-digit identification code 16 is suitably calculated from account code 12, four-digit identification code 14 or

30 three-digit identification code 15 and expiration date 13 based upon a predetermined algorithm (step 40). Five-digit identification code 16 is preferably calculated and encoded

into the magnetic stripe because five-digit identification code 16 provides additional security by not being disclosed on the face of the card (only four-digit code 14 or three-digit code 15 are visible).

After determining identification codes 14, 15 and 16, transaction card 10 is
5   preferably created with an embossed account code 12, embossed expiration date 13, embossed consumer's name 11 and non-embossed card identification codes 14, 15 and 16 (step 42). Particularly, in a preferred embodiment, a four-digit identification code 14 is printed (non-embossed) on the front of card 10 above account code 12, an associated five-digit identification code 16 is encoded into the magnetic stripe and an associated
10 three-digit identification code 15 is printed in the signature panel. One skilled in the art will appreciate that any one of the aforementioned card identification codes 14, 15 and 16 may exist throughout this process alone or in any combination with the other card identification codes. For example, only identification code 14 may appear on the front of the card without any codes on the back of the card or in the magnetic stripe. Moreover,
15 identification codes 14, 15 and 16 may comprise any number of digits, symbols, characters, letters and/or the like and may be located in any location and in any medium on card 10. For example, an identification code may be encoded into an integrated circuit in a smart card embodiment.

Upon printing of transaction cards 10, an embossing file 34 including card
20 identification codes 14, 15 and 16 is created (step 44). Embossing file 34 with associated identification codes 14, 15 and 16 is next uploaded into account database 30 (step 46). In a preferred embodiment, authorization server 26 communicates with, and analyzes the data within, account database 30 (step 48). Alternatively, the use of a Hardware Security Module allows embossing file 34 to provide a simplified, more direct transmission of
25 embossing information to account database 30 without the need for maintenance uploads. In a particularly preferred embodiment, as shown in Figure 4, identification codes are stored in a look-up table within account database 30.

Referring to Figure 3, an exemplary authorization system 20, account database 30 and card creation system 32 is shown. Authorization system 20 is any authorization
30 system suitably configured to authorize a transaction card and notify an input device 22 of the authorization status. One skilled in the art will appreciate that authorization system

20 can be an existing authorization system, such as the Central Authorization System used by American Express, which is re-programed or re-configured to preform the functions of the present invention or is a system specially configured to preform the functions of the present invention. In a preferred embodiment, authorization system 20

5   includes input device 22, network 24 and authorization server 26. Input device 22 is any device suitably configured to accept transaction information and transmit the information for approval. In a preferred embodiment, input device 22 is a telephone, computer, point-of-sale terminal, ATM and/or the like. Input device 22 preferably communicates with network 24, wherein network 24 is any device or software suitably configured to transmit

10 information. In a preferred embodiment, network 24 is a modem, a PSTN, an Internet, an Intranet, a direct link, or any combination thereof.

With continued reference to Figure 3, network 24 provides a communication link between input device 22 and authorization server 26. Authorization server 26 is any device suitably configured to authorize a transaction and/or transaction card and notify

15 input device 22 of the authorization status. In a preferred embodiment, authorization server 26 is a centralized authorization system including transaction account codes. One skilled in the art will appreciate that authorization server 26 can be a centralized database providing authorization information to various input devices 22. Moreover, one skilled in the art will appreciate that authorization server 26 may include any combination of

20 components, software, servers and computers suitably configured to not only authorize transactions and/or transaction cards, but also to provide additional transaction support such as report generation and promotional programs. Authorization server 26 is preferably in communication with, and interrogates, account database 30. One skilled in the art will appreciate that account database 30 can be a separate component, integrated

25 into authorization server 26 or simply software within authorization server 26 or within input device 22. In a preferred embodiment, account database 30 includes a look-up table (see Figure 4), thereby allowing verification of the association between account codes 12 and identification codes 14, 15 and 16.

Referring to Figure 5, when a consumer uses transaction card 10, a clerk, sales

30 representative, merchant, consumer or other authorized person inputs account code 12 and card identification code 14, 15 or 16, along with any other transaction information

- 8 -

such as purchase amount, etc., into input device 22 (step 50). In one embodiment, card identification code 14 or 15 is manually keyed into input device 22. The keyed information is sent via network 24 to authorization server 26 (step 51). Authorization server 26 suitably determines if the data was keyed in or swiped through input device 22 (step 52).

5   In a preferred embodiment, to help determine if the data was keyed or swiped, the keyed data includes different formatting, uses different communication lines, different number of digits in the identification code and/or different header information than information read from the magnetic stripe.

After authorization server 26 determines that the information is manually keyed

10 information, authorization server 26 suitably interrogates account database 30 to determine if the keyed identification code 14 or 15 matches the respective identification number on file for that transaction card (step 54). If the respective identification codes 14 or 15 match, the authorization process proceeds to determine if other authorization parameters are satisfied (step 58). If the respective identification codes 14 or 15 do not

15 match, the transaction is denied and an "invalid Card ID" message is transmitted to the input device 22 (step 60). In an alternative embodiment, if the identification numbers do not correspond, authorization server 26 preferably prompts input device 22 to re-enter the card identification code and the process is repeated. If the numbers do not correspond again, transaction card 10 is denied.

20   When the card is swiped through a POS device 22, the five-digit number previously entered into the magnetic stripe, along with other information, is automatically transmitted to authorization server 26. Authorization server 26 suitably determines that the data originated from a magnetic stripe (step 52) by various methods such as, for example, data format, communication lines from which the data was sent, header information and/or the

25 number—of—digits in the identification code. Authorization server 26 preferably decomposes the five-digit identification code 16 into a four-digit number using a predetermined mathematical algorithm (step 56). In a preferred embodiment, this algorithm is the inverse of the algorithm set forth above used to create the five-digit identification code 16. Alternatively, account database 30 includes five-digit identification

30 codes 16 for each account code 12, thereby eliminating the need to transform the five-digit code 16 to a four-digit code 14. The algorithm is optimally a robust and secure

algorithm which conforms to the Data Encryption Standard. Similar to above, authorization server 26 then suitably interrogates account database 30 to determine if the derived four-digit number 14 matches the four-digit number on file for that transaction card (step 54). If the four-digit numbers match, the authorization process proceeds to

5   determine if other authorization parameters are satisfied (step 58). If the four-digit numbers do not match, the transaction is denied and an "invalid Card ID" message is transmitted to the input device 22 (step 60). In an alternative embodiment, if the numbers do not correspond, authorization server 26 preferably prompts input device 22 to re-swipe the card identification code 16 and the process is repeated. If the numbers do not

10 correspond again, transaction card 10 is denied.

In a further alternative embodiment, the incorporation of card identification code 14 into a particular authorization process is optional depending on the type of transaction card 10 or account code 12 used for the financial transaction. In other words, when authorizing a transaction, the same authorization system 20 may not require a card

15 identification code 14 for particular account codes 12. For example, certain consumers may be enrolled in a promotional program which includes a cardless account without a card identification code 14. As such, while other verification means typically exist, authorization server 26 may not require entry of an identification code or account database 30 may include any suitable automatic authorization for certain ranges of

20 account codes 12, regardless of entry of a card identification code 14.

In a preferred embodiment, account codes 12 are subject to periodic update as new card promotions or new accounts are opened. For security reasons, card identification codes 14, 15 or 16 are preferably only retained in authorization server 26 until authorization or rejection is received by input device 22. Moreover, in a preferred

25 embodiment, card identification codes 14, 15 or 16 are not permanently stored in the input device 22 or the authorization server 26 and are not printed on documents (i.e., receipts, tickets, itineraries, etc.).

Although the invention has been described herein in conjunction with the appended drawings, those skilled in the art will appreciate that the scope of the invention is not so

30 limited. Modifications in the selection, design and arrangement of various components and steps discussed herein may be made without departing from the scope of the

invention as set forth in the claims. Moreover, the present invention may be described herein in terms of functional block components and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware components configured to perform the specified function. For example, the present

5   invention may employ various integrated circuit components, e.g., memory elements, digital signal processing elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more micro-processors or other control devices.

In addition, those skilled in the art will appreciate that the present invention may be

10 practiced in any number of data communication contacts and that the authorization system described herein is merely one exemplary application for the invention. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, training, signal processing and conditioning, and the like. Such general techniques that may be known to those skilled in the art are not

15 described in detail herein.

CLAIMS

1.   A system for authorizing commercial transactions comprising:

a transaction card having an n character account code and an n character identification code, wherein said identification code is not an expiration date and wherein

5 said account code and said identification code have a predetermined logical relationship;

an input device for receiving said account code and said identification code; and,

an authorization computer in communication with said input device, said authorization computer configured to confirm said predetermined relationship between

10 said account code and said identification code.

2.   The system of claim 1, wherein said transaction card is at least one of a credit card, debit card, bank card, charge card and smart card.

3.   The system of claim 1, where in said identification code is unembossed.

4.   The system of claim 1, wherein said account code and said identification

15 code are on the same side of said transaction card.

5.   The system of claim 1, wherein said input device is at least one of a keypad, POS terminal, ATM terminal, computer and telephone.

6.   The system of claim 1, wherein said identification code is at least one of a three-digit number, four-digit number and five-digit number.

20   7.   The system of claim 1, wherein said account code and said identification code are on the same side of said transaction card and said identification code is an unembossed four-digit number located above said account code.

8.   The system of claim 1, wherein said authorization computer is configured to transform said identification code to a second identification code.

9.   The system of claim 1, wherein said authorization computer communicates with an account database and said authorization computer is configured to confirm said

5   predetermined relationship between said account code and said identification code by interrogation of said account database.

10.   A method for authorizing commercial transactions comprising:

keying an n character account code and an n character identification code into an input device, wherein said identification code is not an expiration date and wherein

10   said account code and said identification code have a predetermined logical relationship;

communicating, from said input device to an authorization computer, said account code and said identification code; and,

confirming, at said authorization computer, said predetermined relationship between said account code and said identification code.

15   11.   The method of claim 10, wherein said keying step includes keying said n character account code and said n character identification code into said input device, wherein said input device is at least one of a keypad, POS terminal, ATM terminal, computer and telephone.

12.   The method of claim 10, wherein said keying step includes keying said

20   account code and said identification code which are located on a transaction card, further wherein said account code and said identification code are printed on the same side of said transaction card and said identification code is an unembossed four-digit number located above said account code.
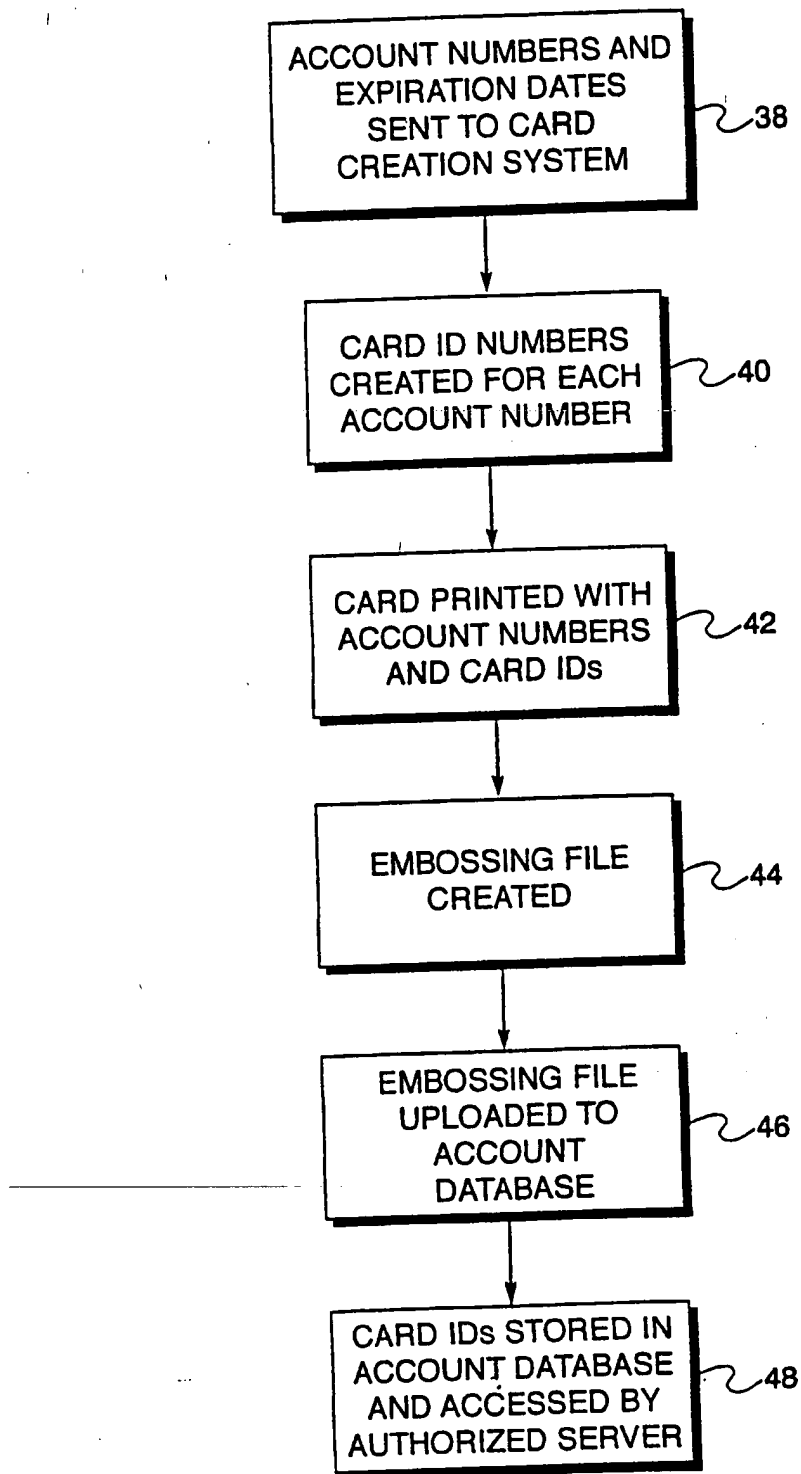
13.   The method of claim 10, further comprising transforming, via said

25   authorization computer, said identification code to a second identification code.

14.   The method of claim 10, further comprising communicating between said authorization computer and an account database and confirming, via said authorization computer, said predetermined relationship between said account code and said identification code by interrogating said account database.

5   15.   A transaction card for authorizing commercial transactions comprising:

an n character account code in a first field;

an n character identification code in a second field, wherein said identification code is not an expiration date;

wherein said account code and said identification code have a

10   predetermined logical relationship;

said transaction card configured to provide, via an input device, said account code and said identification code to an authorization computer, wherein said authorization computer is configured to confirm said predetermined relationship between said account code and said identification code.

15   16.   The system of claim 15, wherein said transaction card is at least one of a credit card, debit card, bank card, charge card and smart card.

17.   The system of claim 15, wherein said account code and said identification code are on the same side of said transaction card and said identification code is an unembossed four-digit number located above said account code.
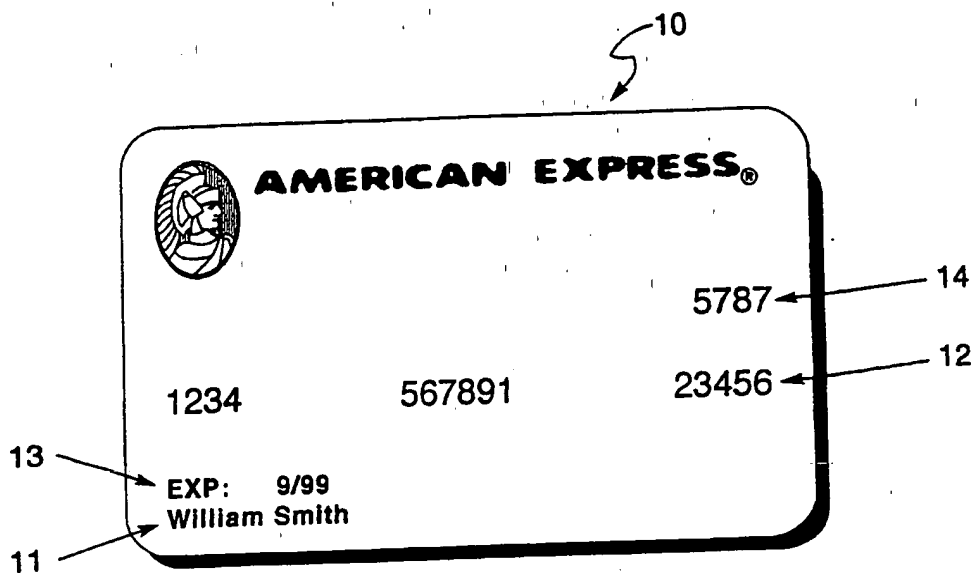
ACCOUNT NUMBERS AND
EXPIRATION DATES
SENT TO CARD
CREATION SYSTEM — 38

↓

CARD ID NUMBERS
CREATED FOR EACH
ACCOUNT NUMBER — 40

↓

CARD PRINTED WITH
ACCOUNT NUMBERS
AND CARD IDs — 42

↓

EMBOSSING FILE
CREATED — 44

↓

EMBOSSING FILE
UPLOADED TO
ACCOUNT
DATABASE — 46

↓

CARD IDs STORED IN
ACCOUNT DATABASE
AND ACCESSED BY
AUTHORIZED SERVER — 48

FIG. 1.

FIG. 2A.

FIG. 2B.

FIG. 3.

INPUT DEVICE

22

NETWORK

24

AUTHORIZATION SEVER

26

20

ACCOUNT DATABASE

30

32

EMBOSSING FILE

CARD CREATION SYSTEM

34
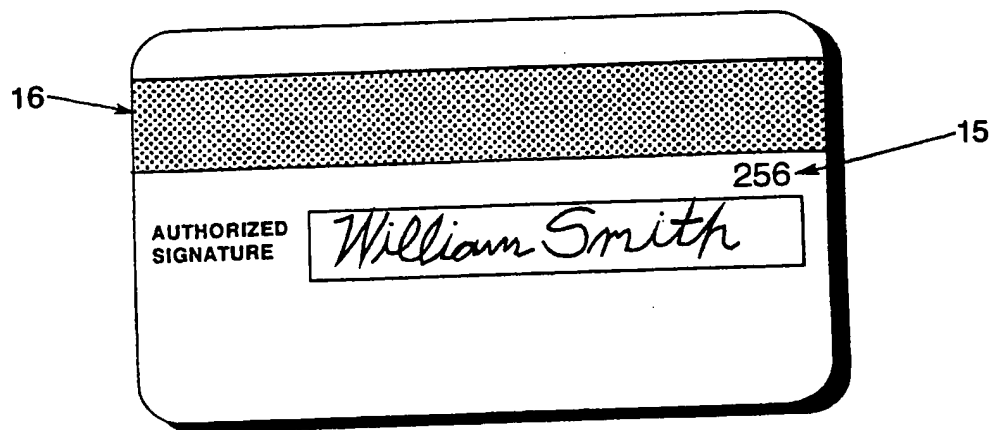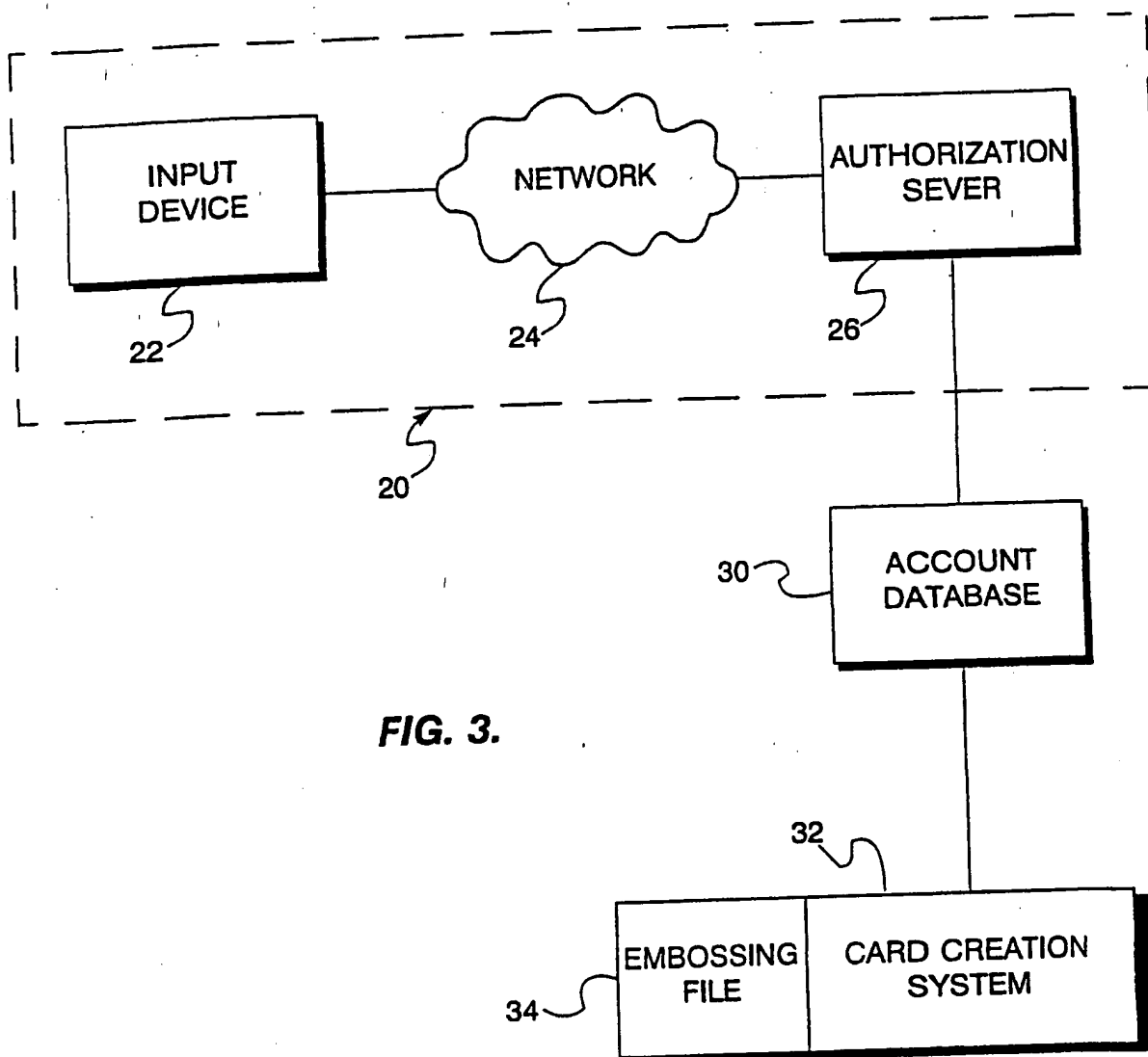
ACCOUNT CODE	EXP. DATE	4-DIGIT ID CODE	3-DIGIT ID CODE	OTHER INFO
1234 567891 11121	1/99	1765	212	
3141 516178 19202	1/00	8274	314	
2122 232435 26278	5/99	5933	103	
3456 789101 12134	7/98	4116	149	
5678 910112 13145	6/99	3821	586	
1617 181920 21222	5/99	9298	567	
"	"	"	"	
"	"	"	"	
"	"	"	"	
"	"	"	"	

FIG. 4.
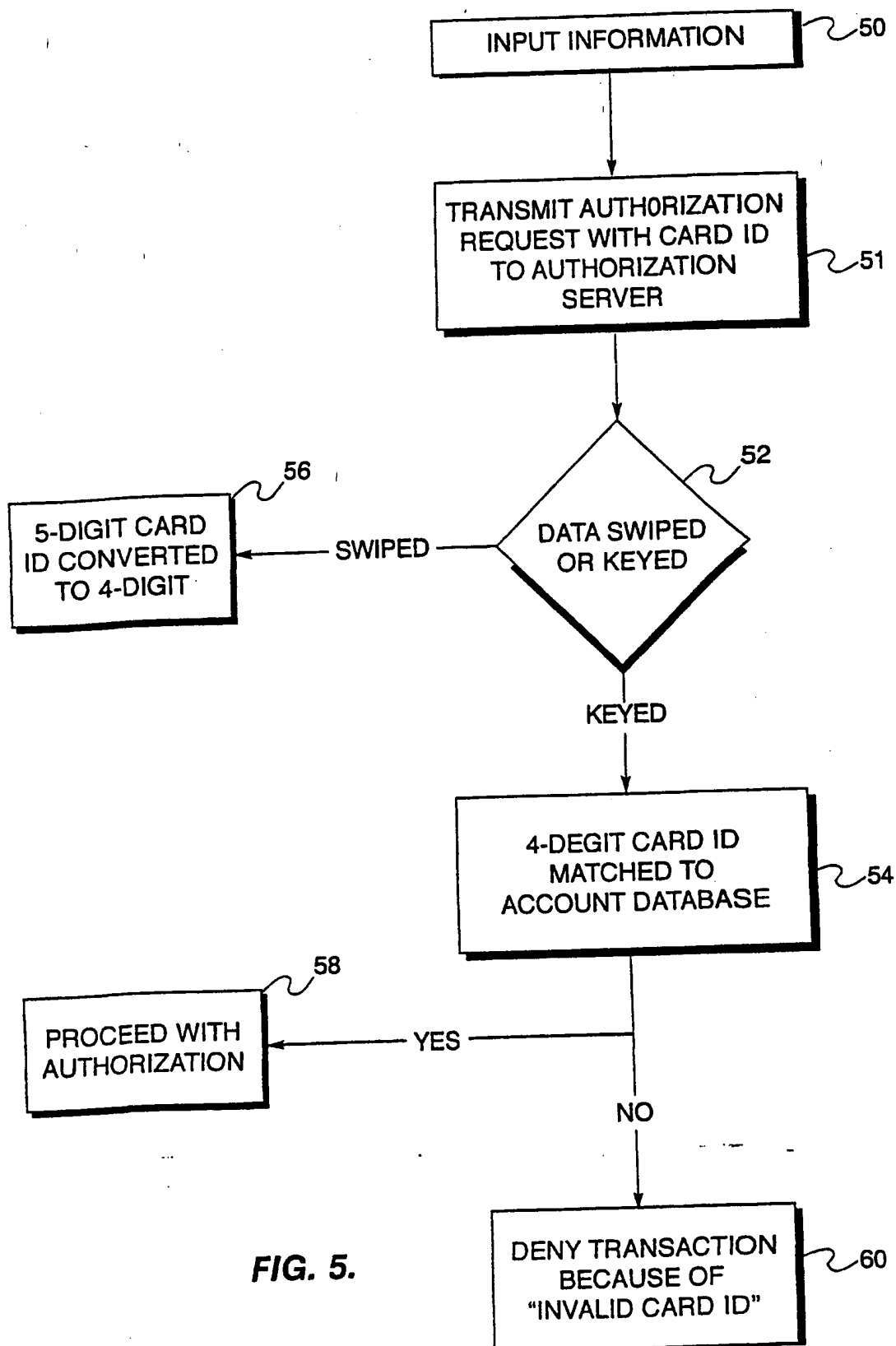
FIG. 5.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US99/25423

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06K 19/06

US CL :235/380, 379, 492, 382.5, 487

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : G06K 19/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

None

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

None

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,734,568 A (Watanabe) 29 March 1988 (29-03-1988), see the entire reference.	1-17
Y	US 4,831,245 A (Ogasawara) 16 May 1989 (16-05-1989), see the entire reference.	1-17
Y	US 5,400,082 A (Kamiya) 21 March 1995 (21-03-1995), see the entire reference.	1-17

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 DECEMBER 1999	10 FEB 2000

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	for Thien Le
Facsimile No. (703) 305-3230	Telephone No. (703) 305-3700

Form PCT/ISA/210 (second sheet)(July 1992)★